Research Paper | Computer Science | E-ISSN No : 2454-9916 | Volume : 3 | Issue : 5 | May 2017

# A REVIEW OF MAC ADDRESS FILTERING AND SPOOFING IN WINDOWS OPERATING SYSTEM

S. Poorana Senthilkumar [1] | C. Kumuthini [1] | P. Dineshkumar [1]

[1] Assistant Professor, Department of Computer Applications, Dr N.G.P Arts and Science College, Coimbatore, Tamil Nadu, India.

## ABSTRACT

MAC (Media Access Control) is a part of data link layer in OSI model, which takes high responsibility to data interchange and connectivity on wireless network. MAC having Filtering option that will consider as white filtering and black filtering, the MAC address can be easily obtained from network traffic. The MAC Address Filtering allows device with specific MAC addresses to connect to any wireless network. This isn't a great security tool because people can easily spoof their MAC addresses. In this paper is a basic idea about MAC address filtering issues and how can prevent the network.

**KEY WORDS:** MAC Address, Filtering, white filtering, black filtering, wireless network.

## INTRODUCTION

All wireless network interface having MAC address, it takes main roll for network device connectivity on the wireless network. Media Access Control (MAC), MAC addresses are also commonly referred to as physical addresses or hardware addresses, because they correspond to a hardware adapter. MAC addresses are used as a network address for IEEE 802 protocol in wireless network connections. This MAC address is Unique 48 bits or 6 bytes length Address in the format of MM:MM:MM:SS: SS: SS. The leftmost 6 digits (24 bits) called a "prefix" is associated with the adapter manufacturer as assigned by an Internet standards body.

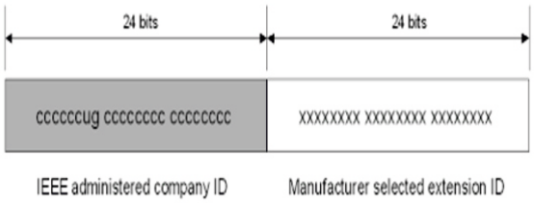


**Figure 1: MAC Address**

The rightmost 3-bytes are serial number assigned by the manufacturer for identifying the device.

### Function of Verification

MAC address filtering is an additional layer in network device. Before letting any device connect to the network, the device's MAC address checked against a list of matching addresses. If the client's address matches one on the router's list, network access permission is granted; otherwise, it's blocked from network connectivity. The list of matching MAC address entries are listed in whitelist.

Mostly router devices include the feature to blacklist or whitelist certain computers or access device based on their MAC address. We can make configure the filter to allow connections from all computers except those included in the blacklist, or restrict access to any computer or access device that isn't included in the whitelist. Whitelists provide most powerful security than blacklists because the router grants access only to selected or approved devices.

### Spoofing MAC Address

Now days there is lot of spoofing technique are available to change the MAC address. The step or technique little bit differs from operating system level. In this section we are discussing how to make spooning in Windows operating system. There are different MAC spoofing techniques one method is to change the MAC address of a router. But not all routers have the ability to change their MAC address. The one having this feature is often referred to as "Clone MAC address". Another technique is to change MAC address on a Cisco router, using the MAC-address command in interface configuration mode.

### WINDOWS operation system

**Method 1:**

This method depends on the type of network interface card

1. Go to Start->Settings->Control Panel and double click on Network and Dial-up Connections.
2. Right click on the NIC you want to change the MAC address and click on properties.
3. Under "General" tab, click on the "Configure" button Click on "Advanced" tab
4. Under "Property section", you should see an item called "Network Address" or "Locally Administered Address", click on it.
5. On the right side, under "Value", type in the New MAC address you want to assign to your NIC. Usually this value is entered without the "-"between the MAC address numbers.
6. Goto command prompt and type in "ipconfig /all" or "net config rdr" to verify the changes. If the changes are not materialized, then use the second method.
7. If successful, reboot your systems

**Method 2:**

The MAC Address can also be changed by registry using following steps:

1. Go to Start -> Run, type "regedt32" to start registry editor. Do not use "Regedit".
2. Go to "HKEY_LOCAL_ MACHINE\ SYSTEM\CurrentControlSet\ Control \Class\{4D36E972-E325-11CE-BFC1 - 08002BE10318}". Double click on it to expand the tree. The subkeys are 4-digit numbers, which represent particular network adapters. You should see it starts with 0000, then 0001,0002, 0003 and so on.(Figure 2)
3. Find the interface you want by searching for the proper "DriverDesc" key.
4. Edit, or add, the string key "NetworkAddress" (has the data type "REG_SZ") to contain the new MAC address.
5. Disable then re-enable the network interface that you changed (or reboot the system).

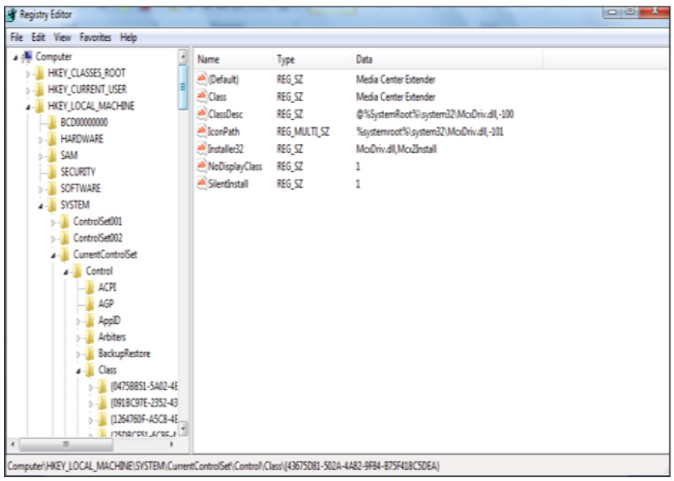


**Figure 2 :Windows Registry Editor**

**Vulnerabilities**

A MAC address is the address hard coded into the Ethernet card. The address changing is possible and very simple in Network. In Some cases it is taken for good effect and in some cases for Bad effect, so some valuable vulnerabilities are pointed out below:-

1. Using of Wireless electronic device (such as PC, LAPTOP , Mobile phone, PDA or ) an unauthorized persons device can access our wireless network.
2. Unknown device is possible to track illegal Internet traffic to a specific IP and to retrieve the name and address of the IP's.
3. MAC address is continuously being sent over Wi-Fi networks, even if they use secure WEP/WPA Encryption.
4. Entry of new device on the network have its MAC address added into the database as an authorized device. Therefore, if you can sniff the MAC address of an existing network node, it is possible to join the network using the MAC address of that node. Mac address filtering provides you effectively no protection against any hacker who has even an ounce of skill.
5. Changing MAC address, the original device information has not been detected and logged by various services such as IDs, Firewalls, DHCP server, Wireless access point etc. to protect user's privacy.
6. Not possible to Protect personal and individual privacy. Some hackers may track users via their MAC addresses. In addition, there are more and more WI-FI wireless connections available these days, and wireless network security and privacy is all about MAC addresses.

## CONCLUSION

In this paper we discussed that MAC address will also be spoofed similarly as IP address spoofing. Spoofing is easily possible because the IEEE 802.11 standard does not provide per-frame source authentication. We have mentioned the easy methods of spoofing the MAC address for windows operating system. The IEEE RAC (Registration Authority Committee) has been working on this issue for the last couple of years. MAC address spoofing is a serious threat to wireless networks. Spoofing is even very easier if a blacklist is in place, the hackers may select (change) another address almost at random to bypass the filter. To get around white lists, hackers use a program called a sniffer, which intercepts data passing through a network; with this we conclude that the most dangerous security issue is in our windows OS. Our windows OS is static but if it will be dynamic then it will resolve our many spoofed network problem. If a MAC is spoofed its entry is made in registry, a dynamic windows OS may have the utility to check its registry after few second if there is any entry with name network address then it should removed from the list. This issues are not only the windows operating system all other operating system also. Anyway we want to prevent network spoofing by any technology. Therefore if the dynamic registry is possible in windows operating system mean the Media Access Control (MAC) not possible to be spoofed.

## REFERENCES

1. IEEE, IEEE Standard 802.11: Wireless LAN Medium Access Control (MAC)and Physical Layer (PHY) Specifications (1999).
2. MAC spoofing available at http://en.wikipedia.org/wiki/
3. M.k.Choi1, R.J. Robles1, C.Hong, T.Kim1, Wireless Network Security:
4. Vulnerabilities,Threats and Countermeasures, International journal of Multimedia and Ubiquitous \ Engineering, Vol.3, No. 3, July, 2008.
5. Payal Pahwa, Gaurav Tiwari and Rashmi Chhabra, "Spoofing Media Access Control (MAC) and its Counter Measures", International Journal of Advanced Engineering & Application, 2010, pp. 186-192.
6. Windows Spoofing available at https://www.lifewire.com/
7. A.William A.Shankar, Narendar, Wan, Y.C. Justin.. your 802.11 wireless networks have no clothes. March 2001